MATTHEW RIGHETTI (SBN#: 121012)
matt@righettilaw.com
JOHN GLUGOSKI (SBN#: 191551)
jglugoski@righettilaw.com
MICHAEL RIGHETTI (SBN#: 258541)
RIGHETTI GLUGOSKI, P.C.
456 Montgomery Street. Suite 1400
San Francisco, CA 94104
Tel: (415) 983-0900
Fax: (415) 397-9005

Attorneys for PLAINTIFFS

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

RICHARD GOSS, an individual and on behalf of others similarly situated,

Plaintiffs,

vs.

SAN FRANCISCO EMPLOYEE RETIREMENT SYSTEM; 10UP INC., and DOES 1-50 inclusive,

Defendants.
_____/

CASE NO.

CLASS ACTION

COMPLAINT

Plaintiff, Richard Goss, brings this Class Action Complaint against San Francisco Employees' Retirement System ("SFERS") and 10UP, Inc., (hereinafter "Defendants") on behalf of himself and all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

1. Defendants receive and retain retiree/member personal and private information, including personally identifiable information ("PII") as defined by California law.

2. On or about February 24, 2020, Defendants were the target of a widespread data breach whereby personal details of thousands of retirees/members were published, disclosed and/or viewed. Plaintiff is informed and believes that the breached, leaked, viewed and/or disclosed data includes personal details such as names, home addresses, dates of birth, designated beneficiary information, 1099-R tax form information, bank routing numbers and SFERS website user names and passwords. Plaintiff is informed and believes, and on that basis alleges, that the information breached, leaked, viewed and/or disclosed was the result of unauthorized access to the pension system vendor's (10Up, Inc.) test data server with the aforementioned information. Hackers accessed and obtained this PII in a form that was unencrypted and unredacted. Because of Defendants' breach,

Defendants' customers' PII is available for criminals to access and abuse. Plaintiff and others similarly situated, as alleged herein, face a lifetime risk of identity theft.

3. This PII breach directly and proximately caused by Defendants' negligent and/or careless acts and omissions and the failure to take reasonable procedures to safeguard and protect the aforementioned PII data. In addition to the failure to prevent the breach, Defendants failed to detect the breach immediately and failed to notify affected individuals/victims within a reasonable time period.

4. To this day, Defendants have not released a vulnerabilities and exposures report.

5. The stolen PII has great value to hackers. On information and belief, over seventy thousand of California residents were affected by this breach.

6. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect its users' PII, (ii) warn users of its inadequate information security practices, and (iii) effectively monitor Defendant's website and ecommerce platform for security vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates several California statutes.

7. Plaintiff and similarly situated customers of Defendants ("Class members")

have suffered injury as a result of Defendants' conduct. These injuries may include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the data breach, including but not limited to lost time, (iv) deprivation of rights they possess under the California Unfair Competition Law (Cal. Bus. & Prof. Code § 17200) and California Consumer Privacy Act (Cal. Civ. Code § 1798.100, *et seq*.); (v) the continued and certainly an increased risk to their PII, which (a) remains accessible to criminals enterprises to access and abuse, and (b) remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

II. PARTIES

8. Plaintiff is a citizen of California residing in San Francisco County. Plaintiff is a retiree and member of the SFERS.

9. Defendant 10UP, Inc., is a Limited Liability Company formed in Rhode Island.

III. JURISDICTION AND VENUE

10. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant. Moreover, Plaintiff is a citizen of California and therefore diverse from 10UP, Inc., which is headquartered in Rhode Island.

11. This Court has personal jurisdiction over Defendants because Defendant 10UP Inc., conducts business in the state of California, and because 10UP, Inc., conducts business in California through its website.

12. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Venue is also proper because the acts occurred in the city and county of San Francisco.

IV. FACTUAL ALLEGATIONS

13. The SFERS is the city workers pension fund, which includes over 74,000 members. The SFERS uses a vendor, 10up Inc. to manage and maintain member PII.

14. Defendants represent and warrant to its members that they are concerned

about PII security.

15. Industry standards include developing and maintaining a security policy that covers all aspects of the business, installing firewalls to protect data, and encrypting PII data that is transmitted over public networks using anti-virus software and updating it regularly.

16. Plaintiff is informed and believes that members' information was accessed, viewed, disclosed and/or sold or is still for sale to criminals. Plaintiff is further informed and believes that unauthorized individuals accessed members' unencrypted unredacted aforementioned PII information and possibly more.

17. The hacking and breaches such as occurred here, are commonly made possible through a vulnerability in a website or its backend content management system. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were collecting, causing customers' PII to be exposed for collection by criminals to be used for nefarious and illegal activities including identity theft schemes.

18. Plaintiff is informed and believes that Defendants should have been made aware of this type of breach – it's been going on for almost a decade and the well-publicized and widespread attacks on other companies, which should have alerted Defendants to the very real and imminent danger facing Defendants'

members.

19. Unfortunately, despite all of the publicly available knowledge of the continued compromises of PII in this manner, Defendants' approach to maintaining the privacy and security of Plaintiff and Class members' PII was negligent, or at the very least, Defendants' did not maintain reasonable security procedures and practices appropriate to the nature of the information to protect their members' valuable PII.

20. PII remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200. Experian reports that a stolen credit or debit card number can sell for $5-110 on the dark web; the *fullz* sold for $30 in 2017. Criminals can also purchase access to entire company data breaches from $900 to $4,500.

21. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on its members' as a result of a breach.

22. Knowing that hackers accessed, viewed and/or stole his PII, and that his PII

may be available for sale on the dark web, has caused Plaintiff stress and anxiety. Plaintiff is greatly concerned about the theft of his PII and identity in general. Now, due to Defendants' misconduct and the resulting data breach, hackers obtained his PII at no compensation to Plaintiff whatsoever. That is money lost for Plaintiff, and money gained for the hackers, who could sell the PII for valuable consideration on the dark web.

V. CLASS ALLEGATIONS

Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 22.

23. Plaintiff brings this nationwide class action pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following class: **All individuals whose PII was compromised in the data breach announced by the SFERS in or about February to June 2020 (the "SFERS Class").**

24. Excluded from the Class are the following individuals and/or entities: Defendants and its parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies,

divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

25. Plaintiff reserves the right to modify or amend the definition of the proposed Class before the Court determines whether certification is appropriate.

26. **Numerosity**: The Classes are so numerous that joinder of all members is impracticable. Defendants have identified thousands of customers whose PII may have been improperly accessed in the data breach, including thousands in California alone, and the Classes are identifiable within Defendants' records.

27. **Commonality**: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class members. These include:

a. Whether and when Defendants actually learned of the data breach and whether their response was adequate;

b. Whether Defendants owed a duty to the Class to exercise due care in collecting, storing, safeguarding and/or obtaining their PII;

c. Whether Defendants breached that duty;

d. Whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiff's and Class members' PII;

e. Whether Defendants acted negligently in connection with the monitoring and/or protecting of Plaintiff's and Class members' PII;

f. Whether Defendants knew or should have known that they did not

employ reasonable measures to keep Plaintiff's and Class members' PII secure and prevent loss or misuse of that PII;

g. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the data breach to occur;

h. Whether Defendants caused Plaintiff and Class members damages;

i. Whether Defendants violated the law by failing to promptly notify class members that their PII had been compromised;

j. Whether Plaintiff and the other Class members are entitled to credit monitoring and other monetary relief;

k. Whether Defendants violated California's Deceptive and Unfair Trade Practices Act by failing to implement reasonable security procedures and practices; and

l. Whether Defendants violated California's California Consumer Privacy Act by failing to maintain reasonable security procedures and practices appropriate to the nature of the PII.

39. **Typicality**: Plaintiff's claims are typical of those of other Class members because all had their PII compromised as a result of the data breach, due to Defendants' misfeasance.

40. **Adequacy**: Plaintiff will fairly and adequately represent and protect the interests of the Class members. Plaintiff's Counsel are competent and experienced in litigating privacy-related class actions.

41. **Superiority and Manageability**: Under 23(b)(3), a class action is superior to other available methods for the fair and efficient adjudication of this controversy

since joinder of all the members of the Class is impracticable. Individual damages for any individual Class member are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendants' misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

42. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because Defendants have acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

43. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiff and the Class members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether Defendants breached a legal duty to Plaintiff and the Class members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether Defendants failed to comply with their own policies and

applicable laws, regulations, and industry standards relating to data security;

d. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach; and

e. Whether Class members are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendants' wrongful conduct.

COUNT I

(Negligence)

(On Behalf of Plaintiff and the Class)

Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 43.

44. Defendants owed a duty to Plaintiff and Class members to exercise reasonable care in obtaining, using, and protecting their PII from unauthorized third parties.

45. The legal duties owed by Defendants to Plaintiff and Class members include, but are not limited to the following:

i. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiff and Class members in its possession;

ii. To protect PII of Plaintiff and Class members in its possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

iii. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiff and Class members of the data breach.

46. In addition, Cal. Civ. Code §1798.81.5 requires Defendants to take

reasonable steps and employ reasonable methods of safeguarding the PII of Class members who are California residents.

47. Defendants' duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the FTC, the unfair practices of failing to use reasonable measures to protect PII by companies such as Defendants.

47. Various FTC publications and data security breach orders further form the basis of Defendants' duty. Plaintiff and Class members are consumers under the FTC Act. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with industry standards.

48. Defendants breached its duties to Plaintiff and Class members. Defendants knew or should have known the risks of collecting and storing PII and the importance of maintaining secure systems, especially in light of the facts that hacks seeking PII were surging in 2018 and on the rise in 2019, and the FBI issued warnings right under Defendants' noses before the breach.

49. Defendants knew or should have known that its security practices did not adequately safeguard Plaintiff's and the other Class members' PII, including, but not limited to, the failure to detect the breach.

50. Through Defendants' acts and omissions described in this Complaint, including Defendants' failure to provide adequate security and its failure to protect the PII of Plaintiff and the Class from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, accessed, and misused, Defendants unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiff's and Class members' PII during the period it was within Defendants' possession and control.

51. Defendants breached the duties it owes to Plaintiff and Class members in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect customers' PII and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards during the period of the data breach (*e.g.,* 10UP, Inc., claims its website is PCI DSS compliant and uses SSL/TLS technology to encrypt customers' order information, such as name, address, and credit card number, during data transmission, but that did not occur here);

c. Failing to act despite knowing or having reason to know that Defendants' systems were vulnerable to E-skimming or similar attacks (*e.g.*, for example, failure to use multi-factor authentication and enhanced system monitoring" which should have been taken beforehand); and

d. Failing to timely and accurately disclose to customers that their PII had been improperly acquired or accessed and was accessed, viewed and/or available for sale to criminals on the dark web.

52. Due to Defendants' conduct, Plaintiff and Class members are entitled to credit monitoring. Credit monitoring is reasonable here. The PII taken can be used

towards identity theft and other types of financial fraud against the Class members. There is no question that this PII was taken by sophisticated cybercriminals, increasing the risks to the Class members. The consequences of identity theft are serious and long-lasting. There is a benefit to early detection and monitoring.

53. Experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately $219 to $329 per year.

54. As a result of Defendants' negligence, Plaintiff and Class members suffered injuries that may include: (i) the lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the data breach, including but not limited to time spent deleting phishing email messages and cancelling credit cards believed to be associated with a compromised account; (iv) the continued risk to their PII, which can remain for sale on the dark web and is in Defendant's possession, subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of customers and former customers in their continued possession; (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the PII compromised as a result of the data

breach for the remainder of the lives of Plaintiff and Class members, including ongoing credit monitoring.

55. These injuries were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiff and the other Class members suffered was the direct and proximate result of Defendants' negligent conduct.

COUNT II
(Declaratory Judgment)
(On Behalf of Plaintiffs and the Class)

Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 55.

56. Plaintiff, therefore, seeks a declaration that (1) each Defendant's existing security measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply with its explicit or implicit contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to

promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendants audit, test, and train its security personnel regarding any new or modified procedures;

d. Ordering that Defendants user applications be segmented by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Ordering that Defendants conduct regular database scanning and securing checks;

f. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Ordering Defendants to purchase credit monitoring services for Plaintiff and Class members for a period of ten years; and

h. Ordering Defendants to meaningfully educate its users about the threats they face as a result of the loss of their PII to third parties, as well as the steps Defendants customers must take to protect themselves.

COUNT III
Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code §17200 – Unlawful Business Practices
(On Behalf of Plaintiff and the Class)

57. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 56.

58. Defendants have violated Cal. Bus. and Prof. Code §17200, *et seq*., by engaging in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200 with respect to the

services provided to the California Class.

59. Defendants engaged in unlawful acts and practices with respect to the services by establishing the sub-standard security practices and procedures described herein; by soliciting and collecting Plaintiffs' and California Class members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiffs' and Class members' PII in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendants to take reasonable methods of safeguarding the PII of Plaintiff and the California Class members.

60. In addition, Defendants engaged in unlawful acts and practices by failing to disclose the data breach to California Class members in a timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82. To date, Defendant has still not provided such information to Plaintiff and the California Class members.

61. As a direct and proximate result of Defendants unlawful practices and acts, Plaintiff and the California Class members were injured and lost money or property, including but not limited to the price received by Defendants for the services, the loss of California Class members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

62. Defendants knew or should have known that its computer systems and data security practices were inadequate to safeguard California Class members' PII and that the risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the California Class.

63. California Class members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq.*, including, but not limited to, restitution to Plaintiffs and California Class members of money or property that Defendants may have acquired by means of its unlawful, and unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of its unlawful and unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

COUNT IV
Violation of California's Unfair Competition Law Cal. Bus. & Prof. Code §17200 – Unfair Business Practices
(On Behalf of Plaintiff and the California Class)

64. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 63.

65. Defendants engaged in unfair acts and practices by establishing the sub-standard security practices and procedures described herein; by soliciting and

collecting Plaintiff's and California Class members' PII with knowledge that the information would not be adequately protected; and by storing Plaintiff's and Class members' PII in an unsecure electronic environment. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and Class members. They were likely to deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to Plaintiff and the Class members outweighed their utility, if any.

66. Defendants engaged in unfair acts and practices with respect to the provision of services by failing to take proper action following the data breach to enact adequate privacy and security measures and protect California Class members' PII from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or substantially injurious to Plaintiff and California Class members. They were likely to deceive the public into believing their PII was securely stored, when it was not. The harm these practices caused to Plaintiff and the Class members outweighed their utility, if any.

67. As a direct and proximate result of Defendants' acts of unfair practices and acts, Plaintiff and the California Class members were injured and lost money or property, including but not limited to the price received by Defendants for the

services, the loss of California Class members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

68. Defendants knew or should have known that its computer systems and data security practices were inadequate to safeguard California Class members' PII and that the risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the California Class.

69. California Class members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiff and California Class members of money or property that the Defendants may have acquired by means of its unfair business practices, restitutionary disgorgement of all profits accruing to Defendants because of its unfair business practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief.

70. Plaintiff and the California Class members reserve the right to amend this Complaint as of right to seek damages and relief under Cal. Civ. Code § 1798.100, *et seq*.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and all Class members, requests judgment against the Defendants and that the Court grant the following:

A. An order certifying the Class as defined herein, and appointing Plaintiff and his Counsel to represent the Class;

B. An order enjoining Defendants from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiff's and Class members' PII;

C. An order instructing Defendants to purchase or provide funds for credit monitoring services for Plaintiff and all Class members;

D. An award of compensatory, statutory, and punitive damages, in an amount to be determined;

E. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

F. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Respectfully Submitted,

DATED: June 5, 2020

RIGHETTI · GLUGOSKI, P.C.

MATTHEW RIGHETTI
Attorney for Plaintiff